Top Three HIPAA Lessons Learned in 2015

Written by
Justin Pope, J.D.
Associate Risk Manager
Professional Risk Management Services, Inc. (PRMS)

1. Encrypt!

Admittedly, this lesson should have been learned quite some time ago. In 2014, one-third of Office of Civil Rights' (OCR) resolution agreements were related to the improper disclosure of protected health information (PHI) due to the theft of an electronic portable device. In 2015, half of OCR's case resolution agreements involved the theft of portable devices. While the inability to safeguard devices in these cases is alarming, even more troubling is the fact that investigated covered entities failed to encrypt their portable devices.

The U.S. Department of Health and Human Services defines encryption as "a method of converting an original message of regular text into encoded text." This past year, St. Elizabeth's Medical Center (SEMC), Cancer Care Group (CCG), and Lahey Clinical Hospital each incurred the wrath of OCR after having unencrypted laptops stolen, agreeing to pay millions in resolution settlements. These breaches could have been avoided by encrypting laptops and making PHI indecipherable to thieves. In recent years, OCR has been fairly vocal about the need encrypt portable devices housing sensitive PHI. Under HIPAA's encryption safe harbor, the loss of encrypted portable devices is not deemed to be a breach. We hope more physicians take advantage of this safe harbor by encrypting in 2016.

2. A "thorough and accurate" risk assessment is a great start.

In 2015 case resolution agreements, OCR consistently noted that investigated covered entities failed to do "thorough and accurate" risk assessments. The Security Rule requires covered entities to engage in a scrupulous analysis of potential threats and vulnerabilities and implement policies and procedures accordingly. For those investigated entities that did make such an assessment, OCR most frequently criticized the scope of the assessment and/or the failure to effectively implement policies that addressed the risks.

Have you determined what type of PHI you store and the manner in which you store it? Do you know who has access to your PHI? These are two questions that would likely need to be addressed in a thorough risk assessment. In November, Triple-S Management Corporation learned this lesson the hard way when they were forced to settle with OCR for $3.5 million. After ending its investigation, OCR found that, among other violations, Triple-S did not conduct an adequate risk assessment and consequently failed to revoke database access rights for two former employees who accessed member names, diagnostic codes, and treatment codes while working for a competitor.

OCR provides a security risk assessment tool here: https://www.healthit.gov/providers-professionals/security-risk-assessment.

3. Technology can help *and hurt.*

Advances in technology have made new software platforms and systems available to practices, streamlining clinical care and enhancing workplace efficiency. However, before using any platform that manages PHI, it is important to understand the way in which the platform stores and protects that data. Discussing the platform with your IT department or IT consultant will be essential because you will need to understand how it works in order to properly assess for threats and vulnerabilities.

Keep in mind that certain platforms, systems, or applications may not have been intended to store PHI, and, as a result, may not meet HIPAA's security standards. In the previously mentioned case resolution agreement involving SEMC, OCR also found that certain SEMC employees wrongfully used an "internet-based document sharing application" to store the PHI of approximately 500 individuals. Covered entities shouldn't assume that any platform is HIPAA compliant. If you are going to use a platform that stores or accesses PHI, the maker of the platform should be able to provide an assurance that the platform is indeed HIPAA compliant and should also be willing to sign a business associate agreement. You might be surprised to find that some widely used platforms may not be HIPAA compliant.